

Extension Complexity of Formal Languages¹

Hans Raj Tiwary
hansraj@kam.mff.cuni.cz
KAM/ITI, Charles University,
Malostranské nám. 25,
118 00 Prague 1, Czech Republic

Abstract

In this article we undertake a study of extension complexity from the perspective of formal languages. We define a natural way to associate a family of polytopes with binary languages. This allows us to define the notion of extension complexity of formal languages. We prove several closure properties of languages admitting compact extended formulations. Furthermore, we give a sufficient machine characterization of compact languages. We demonstrate the utility of this machine characterization by obtaining upper bounds for polytopes for problems in nondeterministic logspace; lower bounds in streaming models; and upper bounds on extension complexities of several polytopes.

Keywords: Extended formulations, formal languages

¹This work was partially supported by grant no. P202-13/201414 of GAČR

1. Introduction

A polytope Q is said to be an extended formulation of a polytope P if P can be described as a projection of Q . Measuring the size of a polytope by the number of inequalities required to describe it, one can define the notion of *extension complexity* of a polytope P – denoted by $\text{xc}(P)$ – to be the size of the smallest possible extended formulation.

Let φ be a boolean formula. Consider the following polytopes:

$$\begin{aligned}\text{SAT} &= \text{conv} \{ \mathbf{x} \mid \mathbf{x} \text{ encodes a satisfiable boolean formula} \} \\ \text{SAT}(\varphi) &= \text{conv} \{ \mathbf{x} \mid \varphi(\mathbf{x}) = 1 \}\end{aligned}$$

The former polytope consists of all strings that encode² satisfiable boolean formulae, while the latter language consists of all satisfying assignments of a given boolean formula. Which of these represents the boolean satisfiability problem *more naturally*?

Reasonable people will agree that there is no correct choice of a natural polytope for a problem. One complication is that there are various kinds of problems: decision, optimization, enumeration, etc, and very similar problems can have very different behaviour if the notion of problem changes.

Several recent results have established superpolynomial lower bounds on the extension complexity of specific polytopes. For example Fiorini et. al [1] showed that polytopes associated with MAX-CUT, TSP, and Independent Set problems do not admit polynomial sized extended formulations. Shortly afterwards Avis and the present author [2] showed that the same holds for polytopes related to many other NP-hard problems. Subsequently Rothvoß [3] showed that even the perfect matching polytope does not admit polynomial sized extended formulation. These results have been generalized in multiple directions and various lower bounds have been proved related to approximation [4, 5, 6] and semidefinite extensions [7, 8, 9].

A few fundamental questions may be raised about such results:

- How does one choose (a family of) polytopes for a specific problem?
- To what extent does this choice affect the relation between extension complexity of the chosen polytope and the complexity of the underlying problem?
- What good are extension complexity bounds anyway³?

The intent of this article is to say something useful (and hopefully interesting) about such problems. In particular, our main contributions are the following:

- We define formally the notion of extension complexity of binary language. Our definition is fairly natural and we do not claim any novelty here. This however is a required step towards any systematic study of problems that admit small extended formulations.
- We define formally what it means to say that a language admits small extended formulation. Again we do not claim novelty here since Rothvoß mentions similar notion in one of the first articles showing existence of polytopes with high extension complexity [10].

²Assume some (arbitrary but fixed) encoding of boolean formulae as binary strings.

³Perfect Matching remains an easy problem despite exponential lower bound on the extension complexity of the perfect matching polytope. What does an exponential lower bound for the cut polytope tell us about the difficulty of the MAX-CUT problem?

- We prove several closure properties of languages that admit compact extended formulations. Some of these results are trivial and some follows from existing results. For a small number of them we need to provide new arguments.
- We prove a sufficient condition in terms of walks on graphs and in terms of accepting Turing Machines, for a language to have polynomial extension complexity. We show how this characterization can be used to prove space lower bounds for non-deterministic streaming algorithms, and also to construct compact extended formulations for various problems by means of a small “verifier algorithm”. We provide some small examples to this end.

2. Background Material and Related Work

2.1. Polytopes and Extended Formulations

A polytope $P \subseteq \mathbb{R}^d$ is a closed convex set defined as intersection of a finite number of inequalities. Alternatively, it can be defined as the convex hull of a finite number of points. Any polytope that is full-dimensional has a unique representation in terms of the smallest number of defining inequalities or points. The *size* of a polytope is defined to be the smallest number of inequalities required to define it. For the purposes of this article all polytopes will be assumed to be full-dimensional. While in doing so, no generality is lost for our discussion, we will refrain from discussing such finer points. We refer the reader to [11] for background on polytopes.

A polytope Q is called an *Extended Formulation* or simply *EF* of a polytope P , if P can be obtained as a projection of Q . The *extension complexity* of a polytope, denoted by $\text{xc}(P)$, is defined to be the smallest size of any possible EF of P .

Extended formulations have a long history of study. Here we refer to only a handful of work that are closely related to this article. For more complete picture related to extended formulations, we refer the reader to the excellent surveys by Conforti et al. [12] and by Kaibel [13] as a point to start.

We will use the following known results related to extended formulations.

Theorem 1 (Balas [14]). *Let P_1 and P_2 be polytopes and let $P = \text{conv}(P_1 \uplus P_2)$, where \uplus denotes the convex hull of the union. Then $\text{xc}(P) \leq \text{xc}(P_1) + \text{xc}(P_2) + 2$.*

2.2. Online Turing machines

In this article we would be interested in *online* variants of Turing machines. Informally speaking, these machines have access to two tapes: an input tape where the head can only move from left to right (or stay put where it is) and a work tape where the work head can move freely. When the machine halts, the final state determines whether the input has been accepted or not. Such machines - like usual Turing machines - can be either deterministic or non-deterministic. For a non-deterministic machine accepting a binary language \mathbf{L} we require that if $\mathbf{x} \notin \mathbf{L}$ then the machine rejects \mathbf{x} for all possible nondeterministic choices, and if $\mathbf{x} \in \mathbf{L}$ then there be some set of non-deterministic choices that make the machine accept \mathbf{L} .

The working of an online Turing machine can be thought of as the working of an online algorithm that makes a single pass over the input and decides whether to accept or reject the input. Natural extensions allow the machine to make more than one pass over the input.

Definition 1. The complexity class $k\text{-NSPACE}(s(n))$ is the class of languages accepted by a k -pass non-deterministic Turing machines using space $s(n)$. Similarly, the complexity class $k\text{-DSPACE}(s(n))$ is the class of languages accepted by a k -pass deterministic Turing machine using space $s(n)$.

The classes 1L and 1NL were introduced by Hartmanis, Mahaney, and Immerman [15, 16] to study weaker forms of reduction. In our terminology the class 1L would be $1\text{-DSPACE}(\log n)$ while the class 1NL would be $1\text{-NSPACE}(\log n)$. The motivation for defining these classes was that if we do not know whether P is different from NP or not, then using a polynomial reduction may not be completely justified in saying that a problem is as hard or harder than another problem, and weaker reductions are probably more meaningful. In any case, these languages have a rich history of study. It is known that non-determinism makes one-pass machines strictly more powerful for $s(n) = \Omega(\log n)$ [17].

2.3. Glued Product of Polytopes

Let $P_1 \subseteq \mathbb{R}^{d_1+k}$ and $P_2 \subseteq \mathbb{R}^{d_2+k}$ be two 0/1 polytopes with vertices $\text{vert}(P_1), \text{vert}(P_2)$ respectively. The *glued product* of P_1 and P_2 where the glueing is done over the last k coordinates is defined to be:

$$P_1 \times_k P_2 := \text{conv} \left\{ \begin{pmatrix} \mathbf{x} \\ \mathbf{y} \\ \mathbf{z} \end{pmatrix} \in \{0, 1\}^{d_1+d_2+k} \left| \begin{pmatrix} \mathbf{x} \\ \mathbf{z} \end{pmatrix} \in \text{vert}(P_1), \begin{pmatrix} \mathbf{y} \\ \mathbf{z} \end{pmatrix} \in \text{vert}(P_2) \right. \right\}.$$

We will use the following known result about glued products.

Lemma 1. [18, 19] Let $P_1 \subseteq \mathbb{R}^{d_1+k}$ and $P_2 \subseteq \mathbb{R}^{d_2+k}$ be two 0/1 polytopes such that the every vertex of P_1 and P_2 contains at most one nonzero coordinate entry among the k -coordinates used for the glueing. Then,

$$\text{xc}(P_1 \times_k P_2) \leq \text{xc}(P_1) + \text{xc}(P_2).$$

3. Polytopes for Formal Languages

Let $\mathbf{L} \subseteq \{0, 1\}^*$ be a language over the 0/1 alphabet. For every natural number n define the set $\mathbf{L}(n) := \{\mathbf{x} \in \{0, 1\}^n \mid \mathbf{x} \in \mathbf{L}\}$. Viewing each string $\mathbf{x} \in \mathbf{L}(n)$ as a column vector, and ordering the strings lexicographically, we can view the set $\mathbf{L}(n)$ as a matrix of size $n \times |\mathbf{L}(n)|$. Thus we are in a position to naturally associate a family of polytopes with a given language and the extension complexity of these polytopes can serve as a natural measure of how hard is it to model these languages as Linear Programs.

That is, one can associate with \mathbf{L} , the family of polytopes $\mathcal{P}(\mathbf{L}) = \{P(\mathbf{L}(1)), P(\mathbf{L}(2)), \dots\}$ with $P(\mathbf{L}(n)) := \text{conv}\{\mathbf{x} \mid \mathbf{x} \in \mathbf{L}(n)\}$. The extension complexity $\text{xc}(\mathcal{P}(\mathbf{L}))$ is then an intrinsic measure of complexity of the language \mathbf{L} .

Extension complexity of Languages

Definition 2. The *extension complexity* of a language \mathbf{L} – denoted by $\text{xc}(\mathbf{L})$ – is defined by $\text{xc}(\mathbf{L}) := \text{xc}(\mathcal{P}(\mathbf{L}))$.

We say that the *extension complexity* of \mathbf{L} , denoted by $\text{xc}(\mathbf{L})$ is $\mathbf{f}(n)$, where $\mathbf{f} : \mathbb{N} \rightarrow \mathbb{R}_+$ is a non-negative non-decreasing function on natural numbers, if for every polytope $P(\mathbf{L}(n)) \in \mathcal{P}(\mathbf{L})$ we have that $\text{xc}(P(\mathbf{L}(n))) = \mathbf{f}(n)$. One can immediately see that this definition is rather useless in its present form since for different values of n , the corresponding polytopes in $\mathcal{P}(\mathbf{L})$ may have extension complexities that are not well described by a simple function. For example, the perfect matching polytope would have no strings of length n if n is not of the form $\binom{r}{2}$ for some even positive integer r . To avoid such trivially pathological problems, we will use asymptotic notation to describe the membership extension complexity of languages.

We will say that $\text{xc}(\mathbf{L}) = \mathcal{O}(\mathbf{f})$ to mean that there exists a constant $c > 0$ and a natural number n_0 such that for every polytope $P(\mathbf{L}(n)) \in \mathcal{P}(\mathbf{L})$ with $n \geq n_0$ we have $\text{xc}(P(\mathbf{L}(n))) \leq c\mathbf{f}(n)$.

We will say that $\text{xc}(\mathbf{L}) = \Omega(\mathbf{f})$ to mean that there exists a constant $c > 0$ and such that for every natural number n_0 there exists an $n \geq n_0$ such that $\text{xc}(P(\mathbf{L}(n))) \geq c\mathbf{f}(n)$. Note the slight difference from the usual Ω notation used in asymptotic analysis of algorithms⁴. The intent here is to be able to say that a polytope family of a certain language contains an infinite family of polytopes that have high extension complexity.

Finally, we will say that $\text{xc}(\mathbf{L}) = \Theta(\mathbf{f})$ to mean that $\text{xc}(\mathbf{L}) = \mathcal{O}(\mathbf{f})$ as well as $\text{xc}(\mathbf{L}) = \Omega(\mathbf{f})$. To give an example of the notation, recent result of Rothvoß[3] proving that perfect matching polytope has high extension complexity would translate in our setting to the following statement:

Theorem. [3] *Let \mathbf{L} be the language consisting of the characteristic vectors of perfect matchings of complete graphs. Then, there exists a constant $c > 1$ such that $\text{xc}(\mathbf{L}) = \Omega(c^n)$.*

One can extend the above notation to provide more information by being able to use functions described by asymptotic notation as well. For example, knowing that the perfect matching polytope for K_n has extension complexity at most $2^{\frac{n}{2}}$ [20] together with Rothvoß' result one could say that the language of all perfect matchings of complete graphs has extension complexity $2^{\Theta(n)}$.

Proposition 1. *For every language $\mathbf{L} \subseteq \{0, 1\}^*$ we have $\text{xc}(\mathbf{L}) \leq \text{xc}(\overline{\mathbf{L}}) \leq 2^n$.*

Proof. The first inequality is trivial. For the last inequality, observe that $\mathbf{L}(n)$ and $\overline{\mathbf{L}}(n)$ has at most 2^n vertices altogether. \square

4. Languages with small extension complexities

Now we are ready to define the class of languages that we are interested in: namely, the languages that have small extension complexities.

Definition 3. \mathcal{CF} is the class of languages admitting Compact extended \mathcal{F} ormulations and is defined as

$$\mathcal{CF} = \{ \mathbf{L} \subseteq \{0, 1\}^* \mid \exists c > 0 \text{ s.t. } \text{xc}(\mathbf{L}) \leq n^c \}$$

⁴This usage, however, is common among number theorists.

4.1. Some canonical examples

For any given boolean formula φ with n variables define the polytope $\text{SAT}(\varphi)$ to be the convex hull of all satisfying assignments and $\text{UNSAT}(\varphi)$ to be the convex hull of all non-satisfying assignments. That is,

$$\begin{aligned}\text{SAT}(\varphi) &:= \text{conv}(\{\mathbf{x} \in \{0,1\}^n \mid \varphi(\mathbf{x}) = 1\}), \\ \text{UNSAT}(\varphi) &:= \text{conv}(\{\mathbf{x} \in \{0,1\}^n \mid \varphi(\mathbf{x}) = 0\})\end{aligned}$$

Let $n \in \mathbb{N}$ and $m = n^2$. For the complete graph K_n define a 3SAT boolean formula φ_m such that $\text{CUT}^\square(K_n)$ – the convex hull of all edge-cuts of the complete graph K_n – is a projection of $\text{SAT}(\varphi_m)$. Consider the relation $\mathbf{x}_{ij} = \mathbf{x}_{ii} \oplus \mathbf{x}_{jj}$, where \oplus is the xor operator. The boolean formula

$$(\mathbf{x}_{ii} \vee \overline{\mathbf{x}}_{jj} \vee \mathbf{x}_{ij}) \wedge (\overline{\mathbf{x}}_{ii} \vee \mathbf{x}_{jj} \vee \mathbf{x}_{ij}) \wedge (\mathbf{x}_{ii} \vee \mathbf{x}_{jj} \vee \overline{\mathbf{x}}_{ij}) \wedge (\overline{\mathbf{x}}_{ii} \vee \overline{\mathbf{x}}_{jj} \vee \overline{\mathbf{x}}_{ij})$$

is true if and only if $\mathbf{x}_{ij} = \mathbf{x}_{ii} \oplus \mathbf{x}_{jj}$ for any assignment of the variables $\mathbf{x}_{ii}, \mathbf{x}_{jj}$ and \mathbf{x}_{ij} .

Therefore we define φ_m (with $m = n^2$) as

$$\varphi_m := \bigwedge_{\substack{i,j \in [n] \\ i \neq j}} \left[\begin{array}{l} (\mathbf{x}_{ii} \vee \overline{\mathbf{x}}_{jj} \vee \mathbf{x}_{ij}) \wedge (\overline{\mathbf{x}}_{ii} \vee \mathbf{x}_{jj} \vee \mathbf{x}_{ij}) \wedge \\ (\mathbf{x}_{ii} \vee \mathbf{x}_{jj} \vee \overline{\mathbf{x}}_{ij}) \wedge (\overline{\mathbf{x}}_{ii} \vee \overline{\mathbf{x}}_{jj} \vee \overline{\mathbf{x}}_{ij}) \end{array} \right]. \quad (1)$$

We will call the family of CNF formulae defined by 1 to be the CUTSAT family. It is easy to see the following.

Lemma 2. $\text{xc}(\text{SAT}(\varphi_m)) = 2^{\Omega(n)}$, where $m = n^2$.

Proof. The satisfying assignments of φ_m when restricted to the variables \mathbf{x}_{ij} with $i \neq j$ are exactly the cut vectors of K_n and every cut vector of K_n can be extended to a satisfying assignment of φ . \square

Lemma 3. $\text{xc}(\text{UNSAT}(\varphi_m)) \leq \mathcal{O}(n^4)$.

Proof. Let φ be a DNF formula with n variables and m clauses. We can show that $\text{xc}(\text{SAT}(\varphi)) \leq \mathcal{O}(mn)$.

If φ consists of a single clause then it is just a conjunction of some literals. In this case $\text{SAT}(\varphi)$ is a face of the n -hypercube and has $\text{xc}(\text{SAT}(\varphi)) \leq 2n$. Furthermore, for DNF formulae φ_1, φ_2 we have that $\text{SAT}(\varphi_1 \vee \varphi_2) = \text{SAT}(\varphi_1) \uplus \text{SAT}(\varphi_2)$. Therefore, using Theorem 1 repeatedly we obtain that for a DNF formula φ with n variables and m clauses $\text{SAT}(\varphi) \leq \mathcal{O}(mn)$. \square

5. Closure properties of compact languages

Now we discuss the closure properties of the class \mathcal{CF} with respect to some common operations on formal languages. The operations that we consider are as follows.

- **Complement** : $\overline{L} = \{\mathbf{x} \mid \mathbf{x} \notin L\}$
- **Union** : $L_1 \cup L_2 = \{\mathbf{x} \mid \mathbf{x} \in L_1 \vee \mathbf{x} \in L_2\}$
- **Intersection** : $L_1 \cap L_2 = \{\mathbf{x} \mid \mathbf{x} \in L_1 \wedge \mathbf{x} \in L_2\}$
- **Set difference** : $L_1 \setminus L_2 = \{\mathbf{x} \mid \mathbf{x} \in L_1 \wedge \mathbf{x} \notin L_2\}$
- **Concatenation** : $L_1 L_2 = \{\mathbf{xy} \mid \mathbf{x} \in L_1 \wedge \mathbf{y} \in L_2\}$
- **Kleene star** : $L^* = L \cup LL \cup LLL \cup LLLL \cup \dots$

Theorem 2. \mathcal{CF} is not closed under taking complement.

Proof. Let Φ be the family of 3CNF formula containing CUTSAT formula for $m = n^2$ and containing some tautology with m variables for all other m . Let \mathbf{L}_{sat} be the language containing satisfying assignments of formulae in this family. Similarly, let $\mathbf{L}_{\text{unsat}}$ be the language containing non-satisfying assignments of formulae in this family.

It is easy to see that $\mathbf{L}_{\text{sat}} = \overline{\mathbf{L}_{\text{unsat}}}$. Now, $\mathbf{L}_{\text{unsat}} \in \mathcal{CF}$ due to Lemma 3 while $\mathbf{L}_{\text{sat}} \notin \mathcal{CF}$ due to Lemma 2. \square

Theorem 3. \mathcal{CF} is closed under taking union.

Proof. Let \mathbf{L}_1 and \mathbf{L}_2 be two languages. Then, $\text{xc}(\mathbf{L}_1 \cup \mathbf{L}_2) \leq \text{xc}(\mathbf{L}_1) + \text{xc}(\mathbf{L}_2) + 2$ (cf. Theorem 1). \square

Theorem 4. \mathcal{CF} is not closed under taking intersection.

Proof. Let \mathbf{L}_1 be a language such that a string $\mathbf{x} \in \mathbf{L}_1$ if and only if it satisfies the following properties.

- $|\mathbf{x}| = (n+1)\binom{n}{2}$ for some natural number n , and
- $\mathbf{x}_{ij(n+1)} = \mathbf{x}_{iji} \oplus \mathbf{x}_{ijj}$ if the characters are indexed as \mathbf{x}_{ijk} with $1 \leq i < j \leq n$, $1 \leq k \leq n+1$.

We claim that $\text{xc}(\mathbf{L}_1) = \mathcal{O}(n^3)$. Indeed $P(\mathbf{L}_1((n+1) \cdot \binom{n}{2}))$ is the product of polytopes

$$P_{ij} = \{\mathbf{x} \in \{0,1\}^{n+1} \mid \mathbf{x}_{n+1} = \mathbf{x}_i \oplus \mathbf{x}_j\}$$

for $1 \leq i < j \leq n$ and $\text{xc}(P_{ij}) = \mathcal{O}(n)$.

Now let \mathbf{L}_2 be a language such that a string $\mathbf{x} \in \mathbf{L}_2$ if and only if it satisfies the following properties.

- $|\mathbf{x}| = (n+1)\binom{n}{2}$ for some natural number n , and
- $\mathbf{x}_{i_1j_1k} = \mathbf{x}_{i_2j_2k}$ for all $k \in [n], i \neq j \in [n]$

Each polytope $P(\mathbf{L}_1((n+1) \cdot \binom{n}{2}))$ is just an embedding of $\square_{n+\binom{n}{2}}$ in $\mathbb{R}^{(n+1)\binom{n}{2}}$ where \square_k is the k -dimensional hypercube. Therefore, $\text{xc}(\mathbf{L}_2) = \mathcal{O}(n^2)$.

Finally, observe that for $m = (n+1)\binom{n}{2}$ the polytope $P((\mathbf{L}_1 \cap \mathbf{L}_2)(m))$ when projected to the coordinates labelled $\mathbf{x}_{ij(n+1)}$ is just the polytope CUT_n^\square (cf. Lemma 2). Therefore, $\text{xc}(\mathbf{L}_1 \cap \mathbf{L}_2) = 2^{\Omega(n)}$ and even though $\mathbf{L}_1, \mathbf{L}_2 \in \mathcal{CF}$, the intersection $\mathbf{L}_1 \cap \mathbf{L}_2 \notin \mathcal{CF}$. \square

Theorem 5. \mathcal{CF} is not closed under taking set difference.

Proof. The complete language $\{0,1\}^*$ clearly belongs to \mathcal{CF} . For any language \mathbf{L} we have $\overline{\mathbf{L}} = \{0,1\}^* \setminus \mathbf{L}$. If \mathcal{CF} were closed under taking set-difference, it would also be closed under taking complements. But as pointed out in Theorem 2, it is not. \square

Theorem 6. \mathcal{CF} is closed under concatenation.

Proof. $P(\mathbf{L}_1\mathbf{L}_2(n))$ is the union of the polytopes $P(\mathbf{L}_1(i)) \times P(\mathbf{L}_2(n-i))$ for $i \in [n]$. Therefore, we have that $\text{xc}(\mathbf{L}_1\mathbf{L}_2) \leq \mathcal{O}(n(\text{xc}(\mathbf{L}_1) + \text{xc}(\mathbf{L}_2)))$. \square

Theorem 7. \mathcal{CF} is closed under taking Kleene star.

Proof. Let $\mathbf{L} \in \mathcal{CF}$. For $0 \leq k \leq n$, consider the polytope P_k defined as

$$P_k := \text{conv} \left(\left\{ \begin{pmatrix} \mathbf{e}_{i+1}^{n+1} \\ \mathbf{0}^i \\ \mathbf{x} \\ \mathbf{0}^{n-i-k} \\ \mathbf{e}_{i+|\mathbf{x}|+1}^{n+1} \end{pmatrix} \in \{0,1\}^{3n+2} \mid \begin{array}{l} \mathbf{x} \in \mathbf{L} \\ |\mathbf{x}| = k \\ 0 \leq i \leq n-k \end{array} \right\} \right)$$

Define $P := \cup_{j=0}^n P_j$. Then, $\text{xc}(P) \leq \sum_{k=0}^n \text{xc}(P_k) \leq \sum_{k=0}^n (n \text{xc}(P(\mathbf{L}(k)))) \leq \mathcal{O}(n^2 \text{xc}(\mathbf{L}))$.

Let S_0 be the face of P defined by the first n coordinates being 0 and the $(n+1)$ -th coordinate being 1. Construct S_{i+1} by taking the glued product of S_i with P over the last $n+1$ coordinates of S_i and the first $n+1$ coordinates of Q .

Take the face R of S_n defined by the last n coordinates being 0 and the $(n+1)$ -th penultimate coordinate being 1. Then, R is an EF for $P(\mathbf{L}^*(n))$. Moreover, $\text{xc}(R) \leq \text{xc}(S_n) \leq (n+1) \text{xc}(P) \leq \mathcal{O}(n^3 \text{xc}(\mathbf{L}))$.

Therefore, $\text{xc}(\mathbf{L}^*) = \mathcal{O}(n^3 \text{xc}(\mathbf{L}))$ and $\mathbf{L}^* \in \mathcal{CF}$. \square

6. Computational power of compact languages

We would like to start the discussion in this section by pointing out that in the class of compact languages is in some sense too powerful. This power comes just from non-uniformity in the definition.

Proposition 2. \mathcal{CF} contains undecidable languages.

It is easy to construct undecidable languages that are in \mathcal{CF} . Take any uncomputable function $\mathbf{f} : \mathbb{N} \rightarrow \{0,1\}$ and define the language \mathbf{L} containing all strings of length n if $\mathbf{f}(n) = 1$ and no strings of length n if $\mathbf{f}(n) = 0$. The extension complexity of \mathbf{L} is $\Theta(2n)$.

At the moment we do not want to start a discussion about controlling the beast that non-uniformity unleashes. Rather we will focus on something more positive. We will show that if a language is accepted by a non-deterministic LOGSPACE online Turing machine, then its extension complexity is polynomial. This brings into fold many non-regular languages already. And as we will see, this characterization allows us to give simple proofs for polynomial extension complexity for some polytopes.

Before we proceed, we would also like to point out that, in the following discussion, the assumption on the input tape being accessed in a one-way fashion is not something one can remove easily. There are languages in LOGSPACE and AC^0 that have exponential extension complexity: for example, the string of all perfect matchings of K_n .

6.1. Polytopes of walks in graphs

Definition 4. Let $D = (V, A)$ be a directed graph with every edge labeled either zero or one. Consider two nodes $u, v \in V$ and a walk ω of length n from u to v . The *signature* of ω – denoted by σ_ω – is the sequence of edge labels along the walk ω . The node u is called the *source* of the walk and the node v the *destination*.

Definition 5. Consider the convex hull of all zero-one vectors of the form (u, σ, v) where u and v are indices of two nodes in D and σ is the signature of some walk of length n from u to v . This polytope – denoted by $P_{\text{markov}}(D, n)$ – is called the *Markovian polytope of D* .

Lemma 4. Let $D = (V, A)$ be directed graph (possibly with self-loops and multiple edges) with every edge labeled either zero or one. Then, $P_{\text{markov}}(D, n)$ has extension complexity at most $2|V| + |A| \cdot n$.

Proof. Let us encode every vertex of D with a zero-one vector of length V such that the unit vector e_i represents vertex i .

Define polytope $P_{\text{trans}} \subset \{0, 1\}^{|V|+1+|V|}$ with $(a, z, b) \in \{0, 1\}^{|V|+1+|V|}$ a vertex of P_{trans} if and only if it encodes a possible transition in D . That is, a and b encode vertices of V , and the coordinate z represents the label of the edge following which one can move from a to b . Since P_{trans} has at most $|E|$ vertices $\text{xc}(P_{\text{trans}}) \leq |E|$.

Let P_0 be the convex hull of (i, e_i) for $i \in V$ and P_f be the convex hull of (e_i, i) for $i \in V$. Observe that the two polytopes are the same except for relabeling of coordinates. Also, $\text{xc}(P_0) = \text{xc}(P_f) \leq |V|$.

Let $P_1 = P_{\text{trans}}$. For $2 \leq i \leq n$, construct the polytope P_i by glueing the last $|V|$ coordinates of P_{i-1} with the first $|V|$ coordinates of P_{trans} . By Lemma 1 we have that $\text{xc}(P_n) \leq |E| \cdot n$.

Finally, let P be the polytope obtained by glueing last $|V|$ coordinates of P_0 with the first $|V|$ coordinates of P_n , and then glueing the last $|V|$ vertices of the result with the first $|V|$ coordinates of P_f . Note that $\text{xc}(P) \leq 2|V| + |E| \cdot n$.

To complete the proof, notice that P is an extended formulation for $P_{\text{markov}}(D, n)$. In particular, projecting out every coordinate except the ones corresponding to the source node in P_0 , the ones corresponding to the destination node in P_f , and ones that correspond to the z coordinates in all the copies of P_{trans} produces exactly the vertices of $P_{\text{markov}}(D, n)$. The z -coordinate corresponding to the i -th copy of P_{trans} corresponds to the i -th index of signatures in the vectors in $P_{\text{markov}}(D, n)$. \square

6.2. Polytopes for Online Turing Machines

Lemma 5. Let $L \in k\text{-NSPACE}(s(n))$. Then, $L \in 1\text{-NSPACE}(\mathcal{O}(ks(n)))$.

Proof. Let M_n be the Turing machine that accepts strings of length n . We will simulate M_n using a multi-tape single pass nondeterministic Turing machine called the simulator S . S is supplied with k work tapes. S starts by guessing the initial work state of M_n at the start of i -th pass and writing them on the i -th work tape. S then simulates (using extra space on each work tape) each of the passes independently starting from their respective initial configuration. Once the entire input has been scanned, the simulator verifies that the work space of M_n on the i -th tape at the end of the pass matches the guess for the initial content for the $(i + 1)$ -th tape. S will accept only if the last tape is in an accepting state.

To store the content of work tape and the current state, S needs $s(n) + o(s(n))$ space for each pass. Thus S uses a single pass and total space of $ks(n)(1 + o(1))$. \square

Thus for our purposes it suffices to restrict our attention to single pass TMs.

Definition 6. The *configuration graph* for input of length n for a given one-pass Turing machine (deterministic or non-deterministic) is constructed as follows. For each fixed n , consider the directed graph whose nodes are marked with a label consisting of $s(n) + \lceil \log(s(n)) \rceil$ characters. The labels encode the complete configuration of the Turing machine: the content of the

worktape and head position on the worktape. We make directed edges between two nodes u and v if the machine can reach from configuration u to configuration v by a sequence of transitions with exactly one input bit read in between. The directed edge is labeled by the input bit read during this sequence of transition.

Finally, we add two special nodes: a start node with a directed edge to each possible starting configuration of the machine, and a finish node with a directed edge from each possible accepting configuration. Each of these directed edges are labeled by zero.

Lemma 6. *The configuration graph for input of length n for a one-pass Turing machine has $\mathcal{O}(2^{s(n)}s(n))$ nodes. If the Turing machine is non-deterministic, this graph has $\mathcal{O}(4^{s(n)}(s(n))^2)$ edges. If the Turing machine is deterministic then this graph has $\mathcal{O}(2^{s(n)}s(n))$ edges.*

Proof. The bound for number of nodes is clear from the construction of the configuration graph. We can have at most two transition edges between any two (possibly non-distinct) nodes: one corresponding to reading a zero on the input tape, and one corresponding to reading a one. Therefore, asymptotically the configuration graph can have number of edges that is at most square of the number of nodes.

For deterministic Turing machine, each node in the configuration graph has exactly two outgoing edges (possibly to the same node). Therefore the number of edges is asymptotically the same as the number of vertices. \square

Now Lemma 4 can be used to bound the extension complexity of language accepted by one-pass machines.

Theorem 8. *Let $L \in 1\text{-NSPACE}(s(n))$. Then, $\text{xc}(L) = \mathcal{O}(4^{s(n)}(s(n))^2 \cdot n)$.*

Proof. Let $L \in 1\text{-NSPACE}(s(n))$ be a language. That is, there exists a Turing machine that when supplied with a string on the one-way input tape uses at most $s(n)$ cells on the worktape, makes a single pass over the input and then accepts or rejects the input. If the input string is in L , some sequence of non-deterministic choices lead the machine to an accepting state, otherwise the machine always rejects.

The length- n strings that are accepted by such a Turing machine correspond exactly to the signatures of length $n + 2$ walks on the corresponding configuration graph D . The first and the last character of these strings is always zero. Therefore, an extended formulation for $P(L(n))$ is obtained by taking the face of $P_{\text{markov}}(D, n + 2)$ corresponding to walks that start and the start node and finish at the finish node. By Lemma 4 $P_{\text{markov}}(D, n + 2)$ has extension complexity $\mathcal{O}(4^{s(n)}(s(n))^2 \cdot n)$, and so does the desired face. \square

If L is accepted by a one-pass deterministic TM then one can do better because the configuration graph has fewer edges.

Theorem 9. *Let $L \in 1\text{-DSPACE}(s(n))$. Then, $\text{xc}(L) = \mathcal{O}(2^{s(n)}s(n) \cdot n)$.*

6.3. Extensions for multiple-pass machines

Theorem 10. *Let $L \in p\text{-NSPACE}(s(n))$. Then, $\text{xc}(L) = 2^{\mathcal{O}(p(n)s(n))}n$.*

Proof. This follows immediately from Lemma 5 and Theorem 8. \square

Theorem 11. *Let \mathcal{M} be a (not necessarily uniform) family of deterministic online Turing machines. Let the number of passes and the space used by the family be bounded by functions, $p(n), s(n)$ respectively. Let $L(\mathcal{M})$ be the language accepted by \mathcal{M} . Then, $\text{xc}(L(\mathcal{M})) \leq 2^{\mathcal{O}(p(n)s(n))}_n$.*

Corollary 1. *If L is accepted by a fixed-pass non-deterministic LOGSPACE Turing machine then $L \in \mathcal{CF}$.*

We end this section with the following remark. For a language to be compact (that is, to have polynomial extension complexity), it is sufficient to be accepted by an online Turing machine (deterministic or not) that requires only logarithmic space. However, this requirement is clearly not necessary. This can be proved by contradiction: Suppose that the condition is necessary. Then the class of compact languages must be closed under taking intersection. (Simply chain the two accepting machines and accept only if both do). Since we have already established (cf. Theorem 4) that the class of compact languages is not closed under taking intersection, we have a contradiction.

7. Applications

7.1. Polytopes of certificates: The nondeterministic LOGSPACE class

Traditionally the most natural polytope associated with a given problem instance is the convex hull of certificates for that instance. For example, the CUT polytope of a graph is the convex hull of all edge-cuts, the perfect matching polytope of a graph is the convex hull of all perfect matchings, etc. This motivates the following definition of natural polytopes associated with problems.

Definition 7. Let $L \subseteq \{0, 1\}^*$ be a language and let M be a verifier for certificates for L . For any instance $\mathbf{x} \in \{0, 1\}^n$ the L_M -polytope of \mathbf{x} – denoted by $P_{(L,M)}(\mathbf{x})$ – is defined to be the convex hull of all string $\mathbf{y} \in \{0, 1\}^{q(n)}$ such that $M(\mathbf{x}, \mathbf{y}) = 1$ where $M(\mathbf{x}, \mathbf{y})$ denotes the output of M when provided with \mathbf{x} and \mathbf{y} on two input tapes.

Certificate based definition of the class NP is perhaps known to everyone who took an undergraduate course in computer science, where the certificates are required to be checkable in polynomial time. A less well known certificate based definition is that of the class NL: the class of languages accepted by nondeterministic logspace Turing machines.

Definition 8 ([21]). A language $L \subseteq \{0, 1\}^*$ is in NL iff there exists a deterministic logspace Turing machine M and a polynomial function $q(\cdot)$ such that

$$\mathbf{x} \in L \iff \exists \mathbf{u} \in \{0, 1\}^{q(|\mathbf{x}|)} \text{ and } M(\mathbf{x}, \mathbf{u}) = 1,$$

where \mathbf{u} is given on a special tape that can be read only from left to right, and $M(\mathbf{x}, \mathbf{u})$ denotes the output of M when \mathbf{x} is placed on the input tape and \mathbf{u} is placed on the one-way tape, and M uses at most $\mathcal{O}(\log |\mathbf{x}|)$ space on its read/write work tape on every input \mathbf{x} .

Let $L \subseteq \{0, 1\}^*$ be a language in NL and let M be the Turing machine that accepts certificates of L as in the previous definition. Then, for each fixed input \mathbf{x} the set of certificates is accepted by a one-pass logspace Turing machine and therefore their convex hull has extension complexity upper bounded by a polynomial with the degree of the polynomial depending on the constant of the logspace use of the work tape by M . Therefore, we have the following:

Theorem 12. Let $L \in \text{NL}$ be a language and let M be the Turing machine accepting certificates of L as in Definition 8. For any instance $\mathbf{x} \in \{0,1\}^n$ the polytope $P_{(L,M)}(\mathbf{x}) = \text{conv}\{\mathbf{y} \in \{0,1\}^{q(n)} \mid M(\mathbf{x}, \mathbf{y}) = 1\}$ has polynomial extension complexity.

7.2. Streaming lower bounds

Reading Theorem 10 in converse immediately yields lower bounds in the streaming model of computation. We illustrate this by an example.

Example 1. We know that the perfect matching polytope of the complete graph K_n has extension complexity $2^{\Omega(n)}$. Any $p(n)$ -pass algorithm requiring space $s(n)$, that correctly determines whether a given stream of $\binom{n}{2}$ is the characteristic vector of a perfect matching in K_n , must have $p(n)s(n) = \Omega(n)$. This bound applies even to non-deterministic algorithms.

In fact Lemma 4 provides an even stronger lower bound.

Definition 9. Let $L \subseteq \{0,1\}^n$ be a language. L is said to be online μ -magic if there exists a Turing machine T that accepts L with the following oracle access. On an input of length n on the one-way input tape, the machine T scans the input only once. At any time (possibly multiple times) during the scanning of the input, T may prepare its working tape to describe⁵ any function $\mathbf{f} : \{0,1\}^{\mu(n)} \rightarrow \{0,1\}^{\mu(n)}$ and a particular input \mathbf{x} and invoke the oracle that changes the contents of the work-tape to $\mathbf{f}(\mathbf{x})$. The machine must always reject strings not in L . For strings in L there must be some possible execution resulting in accept.

Notice that the working of even such a machine can be encoded in terms of the configuration graph where the transitions may depend arbitrarily but in a well-formed way on the contents of the work-tape.

Theorem 13. If the set of characteristic vectors of perfect matchings in K_n are accepted by an online μ -magic Turing machine, then $\mu(n) = \Omega(n)$.

Thus we see that extension complexity lower bounds highlight deep limitations of the streaming model: even powerful oracles do not help solve in sublinear space problems that are LOGSPACE solvable if the one-way restriction on the input is removed.

7.3. Upper bounds from online algorithms

Parity Polytope

As an example, consider the language containing strings where the last bit indicates the parity of the previous bits. This language can be accepted by a deterministic LOGSPACE turing machine requiring a single pass over the input and a single bit of space. Therefore, the parity polytope has extension complexity $\mathcal{O}(n)$.

The parity polytope is known to have extension complexity at most $4n - 4$ [22].

⁵The description is required only to identify the function uniquely and need not be explicit.

Integer Partition Polytope

For non-negative integer n the Integer Partition Polytope, IPP_n , is defined as $\text{IPP}_n := \text{conv}\{x \in \mathbb{Z}_+^n \mid \sum_{k=1}^n kx_k = n\}$.

It is known that $\text{xc}(\text{IPP}_n) = \mathcal{O}(n^3)$ [23].

Consider the polytope in $\mathbb{R}^{\lceil \log n \rceil \times n}$ that encodes each x_i as a binary string. For example, for $n = 4$ the vector $(2, 1, 0, 0)$ is encoded as $(1, 0, 0, 1, 0, 0, 0, 0)$. This polytope is clearly an extended formulation of the Integer Partition Polytope. Call this polytope BIPP_n . The following single pass deterministic algorithm accepts a string $(x_1, x_2, \dots, x_n) \in \{0, 1\}^{\lceil \log n \rceil \times n}$ if and only if the string represents a vertex of BIPP_n .

```

Data: Binary string of length  $n \lceil \log n \rceil$ 
Result: Accept if the input encodes a vertex of the  $\text{BIPP}_n$ 
 $s = 0$ ;  $i = 0$ ;  $l = 0$ ;
while  $i < n$  do
     $b = \text{read\_next\_bit}$ ;
    if  $(s + (i + 1)2^l b) > n$  then
        reject;
    else
         $s = (s + (i + 1)2^l b)$ ;
         $l = (l + 1) \% \lceil \log n \rceil$ ;
        if  $l == 0$  then
             $i++$ ;
        end
    end
end
if  $s == n$  then
    accept;
else
    reject;
end

```

Algorithm 1: One pass algorithm for accepting vertices of BIPP_n .

The above algorithm together with Theorem 9 shows that $\text{xc}(\text{IPP}_n) \leq \text{xc}(\text{BIPP}_n) \leq \mathcal{O}(n^3 \log^2 n)$.

Knapsack Polytopes

For a given sequence of (non-negative) integers $(a, b) = (a_1, a_2, \dots, a_n, b)$, the Knapsack polytope $KS(a, b)$ is defined as $KS(a, b) := \{x \in \{0, 1\}^n \mid \sum_{i=1}^n a_i x_i \leq b\}$.

The Knapsack polytope is known to have extension complexity super-polynomial in n . However, optimizing over $KS(a, b)$ can be done via dynamic programming in time $\mathcal{O}(nW)$ where W is the largest number among a_1, \dots, a_n, b .

Suppose the integers a_i, b are arriving in a stream with a bit in between indicating whether $x_i = 0$ or $x_i = 1$. With a space of W bits, an online Turing machine can store and update $\sum_{i=1}^n a_i x_i$. At the end, it can subtract b and accept or reject depending on whether the result is 0 or not. Any overflow during intermediate steps can be used to safely reject the input. Therefore, the extension complexity of the Knapsack polytope is $\mathcal{O}(nW \log W)$. Note however the extension obtained this way is actually an extended formulation of a polytope encoding all the instances together with their solutions.

Languages in co-DLIN

Let \mathbf{L} be a language such that $\overline{\mathbf{L}}$ is generated by a deterministic linear grammar [24]. The following was proved by Babu, Limaye, and Varma [25].

Theorem 14 (BLV). *Let $\mathbf{L} \in \text{DLIN}$. Then there exists a probabilistic one-pass streaming algorithm using $\mathcal{O}(\log n)$ space that accepts every string in \mathbf{L} and rejects every other string with probability at least $1/n^c$.*

Using the above algorithm together with Theorem 10 we get the following.

Proposition 3. *If $\mathbf{L} \in \text{DLIN}$, then $\overline{\mathbf{L}} \in \mathcal{CF}$.*

8. Conclusion and Outlook

We have initiated a study of extension complexity of formal languages in this article. We have shown various closure properties of compact languages. This is only a first step in what we hope will be a productive path. We have proved a sufficient machine characterization of compact languages in terms of acceptance by online Turing machines. This property is clearly not necessary. What – in terms of computational complexity – characterizes whether or not a language can be represented by small polytopes? We do not know (yet).

References

References

- [1] S. Fiorini, S. Massar, S. Pokutta, H. R. Tiwary, R. de Wolf, Exponential lower bounds for polytopes in combinatorial optimization, *J. ACM* 62 (2) (2015) 17. doi:10.1145/2716307.
- [2] D. Avis, H. R. Tiwary, On the extension complexity of combinatorial polytopes, *Math. Program.* 153 (1) (2015) 95–115. doi:10.1007/s10107-014-0764-2.
- [3] T. Rothvoß, The matching polytope has exponential extension complexity, in: *Symposium on Theory of Computing, STOC 2014, New York, NY, USA, May 31 - June 03, 2014*, 2014, pp. 263–272. doi:10.1145/2591796.2591834.
- [4] G. Braun, R. Jain, T. Lee, S. Pokutta, Information-theoretic approximations of the non-negative rank, *ECCC:2013*-158.
- [5] S. Chan, J. Lee, P. Raghavendra, D. Steurer, Approximate constraint satisfaction requires large LP relaxations, *FOCS'13* (2013).
- [6] G. Braun, S. Fiorini, S. Pokutta, D. Steurer, Approximation Limits of Linear Programs (Beyond Hierarchies), in: *Proc. FOCS 2012, 2012*, pp. 480–489.
- [7] H. Fawzi, P. Parrilo, Exponential lower bounds on fixed-size psd rank and semidefinite extension complexity, *arXiv:1311.2571* (2013).
- [8] J. Briët, D. Dadush, S. Pokutta, On the existence of 0/1 polytopes with high semidefinite extension complexity, *Math. Program.* 153 (1) (2015) 179–199. doi:10.1007/s10107-014-0785-x.
- [9] T. Lee, D. O. Theis, Support-based lower bounds for the positive semidefinite rank of a nonnegative matrix, *arXiv:1203.3961* (2012).
- [10] T. Rothvoß, Some 0/1 polytopes need exponential size extended formulations, *Math. Program.* 142 (1-2) (2013) 255–268. doi:10.1007/s10107-012-0574-3.
- [11] G. M. Ziegler, *Lectures on polytopes*, Vol. 152 of *Graduate Texts in Mathematics*, Springer-Verlag, Berlin-Heidelberg-New York-London-Paris-Tokyo-Hong Kong-Barcelona-Budapest, 1995.
- [12] M. Conforti, G. Cornuéjols, G. Zambelli, Extended formulations in combinatorial optimization, *Annals OR* 204 (1) (2013) 97–143.

- [13] V. Kaibel, Extended formulations in combinatorial optimization, *Optima* 85 (2011) 2–7.
- [14] E. Balas, Disjunctive programming: Properties of the convex hull of feasible points, *Discrete Applied Mathematics* 89 (1-3) (1998) 3–44. doi:10.1016/S0166-218X(98)00136-X.
- [15] J. Hartmanis, N. Immerman, S. R. Mahaney, One-way log-tape reductions, in: 19th Annual Symposium on Foundations of Computer Science, Ann Arbor, Michigan, USA, 16-18 October 1978, 1978, pp. 65–72. doi:10.1109/SFCS.1978.31.
- [16] Hartmanis, Mahaney, Languages simultaneously complete for one-way and two-way log-tape automata, *SICOMP: SIAM Journal on Computing* 10.
- [17] Szepietowski, Weak and strong one-way space complexity classes, *IPL: Information Processing Letters* 68.
- [18] F. Margot, Composition de polyèdres combinatoires: une approche par projection, Ph.D. thesis, École polytechnique fédérale de Lausanne (1994).
- [19] M. Conforti, K. Pashkovich, The projected faces property and polyhedral relations, *Mathematical Programming* (2015) 1–12doi:10.1007/s10107-015-0882-5.
- [20] Y. Faenza, S. Fiorini, R. Grappe, H. R. Tiwary, Extended formulations, nonnegative factorizations, and randomized communication protocols, *Math. Program.* 153 (1) (2015) 75–94. doi:10.1007/s10107-014-0755-3.
- [21] S. Arora, B. Barak, *Computational Complexity - A Modern Approach*, Cambridge University Press, 2009.
- [22] R. Carr, G. Konjevod, Polyhedral combinatorics, in: H. G (Ed.), *Tutorials on Emerging Methodologies and Applications in Operations Research*, Vol. 76 of International Series in Operations Research & Management Science, Springer New York, 2005, pp. 2–1–2–46.
- [23] S. Onn, V. A. Shlyk, Some efficiently solvable problems over integer partition polytopes, *Discrete Applied Mathematics* 180 (2015) 135–140.
- [24] C. de la Higuera, J. Oncina, Inferring deterministic linear languages, in: *Computational Learning Theory, 15th Annual Conference on Computational Learning Theory, COLT 2002, Sydney, Australia, July 8-10, 2002, Proceedings, 2002*, pp. 185–200. doi:10.1007/3-540-45435-7_13.
- [25] A. Babu, N. Limaye, J. Radhakrishnan, G. Varma, Streaming algorithms for language recognition problems, *Theor. Comput. Sci.* 494 (2013) 13–23. doi:10.1016/j.tcs.2012.12.028.